Efficient Image Cipher using 2D Logistic Mapping and Singular Value Decomposition

Mohammed A. AlZain
Department of Information Technology
College of Computers and Information Technology, Taif University
P.O. Box 888, Al-Hawiya-Taif, 21974, KSA

Abstract—The research paper proposes an efficient image cryptosystem that depends on the utilization of two dimensional (2D) chaotic logistic map (CLM) and singular value decomposition (SVD). The encryption process starts by a confusion stage through applying the 2D-CLM to the input plainimage. Then, the resulted logistic transformed image is then decomposed using the SVD technique into three ciphered components; the horizontal, vertical, and diagonal components. The ciphered horizontal, vertical, and diagonal components are then transmitted to the destination which applies a reverse procedure to reconstruct the original plainimage. A matrix of encryption quality tests are performed for investigating the proposed 2D-CLM based SVD image cipher. The obtained test results confirmed and ensured the efficiency of the proposed 2D-CLM based SVD image cipher.

Keywords—Image cipher; 2D-CLM; SVD

I. INTRODUCTION

Recently, the unexpected growing in digital technology field witnessed a lot of attention. And this raises and makes the security issues of the data a critical important task especially during the transmission of sensitive data like images, audios, and videos [1-4]. Images may be utilized in different fields like medical, military, and communication fields, the images may carry important valuable information and may be shared over communication networks, so; it becomes a serious issue to maintain them secured as possible against all probable potential attacks. Plenty of works have been done in recent years and resulted in a many studies on image encryption [5-10].

Several image encoding methods were done and founded in literature like ones that depends on classical encryption like Advanced Encryption Standard (AES), Data Encryption Standard (DES), Double-DES, TDES, and International Data Encryption Algorithm (IDEA) [11-15]. Such techniques does not provide a satisfactory outcomes because of image intrinsic characteristics like huge bulky capacity, high correlation, and redundancy [16-19].

On contrast, many reported methods in literature uses different transformations like Fractional Fourier Transform (FrFT) for image encoding which may be considered as a generalization of FT [20]. Other transformations that are actually utilized in image encryption include Discrete Wavelet transform (DWT) [21], Fractional Wavelet packet (FWP) [22], and 2D-CLM [23-24]. An image cryptosystem that utilizes a multi-channel/multi-stage FrFT is given in [25]. In [26], the authors presented a proposed an image cipher that performs encryption using an iterative FrFT. A color image cipher which applies FWP is presented in [22]. In [27], a color image cipher is proposed that employed encryption in dual FrFT-WT using random phases. In [28], a color image cipher that employed FrFT in conjunction with DWT is presented. In [29], a secure color image cipher which employed a DWT and SVD is proposed. In [30], an image encoding which utilizes SVD and AT in FrFT is presented. This method works as follows; the plainimage is firstly transformed with FrFT and the transformed image is decomposed with SVD into three components. The three components are AT transformed with different iterations, which resulted in the three ciphered images. In decryption procedure, the three ciphered images are inverse AT transformed using the iterations number and the three components are correctly multiplied. Also, uses the inverse FrFT with corrected parameters to achieve the correct decrypted image.

The 2D-CLM can be employed for pixel shuffling for several many image encryption methods [23]. The other method that may be utilized for improving security is the SVD in which the plainimage is decomposed into three components. Such components with the multiplication order are required during decryption and hence may serve as an additional keys.

The main objective of this study is to present an efficient and secure image cipher method for transmitting over secure/unsecure communication network. At encoder end, the encryption process starts by a confusion stage through applying the 2D-CLM to the input plainimage. Then, the resulted logistic transformed image is then decomposed using the SVD technique into three ciphered components; the horizontal, vertical, and diagonal components. At destination, with the knowledge of parameters value, it is easy to retrieve the plainimage from the three ciphered images.

The paper reminder is marshaled as follows: Sect. II provides necessary background regarding the 2D-CLM and the SVD. Sect. III is dedicated for describing in details the proposed 2D-CLM based SVD image cipher. Experimental test results and the analysis of 2D-CLM based SVD image cipher are given in Sect. IV. Sect. V concludes the proposed 2D-CLM based SVD image cipher.
II. BACKGROUND

This section presents the fundamental tools which the proposed image cryptosystem depends on. These tools include the 2D-CLM and the SVD.

A. 2D-CLM

The chaotic logistic is based on several control parameters and this makes it commonly applied in chaos based encryption applications. This is because it is sensitive regarding to initial conditions. The 2D-CLM is derived from the 1D-CLM.

The 1D-CLM can be considered as a simple model that provides a chaotic manner and it can be represented mathematically as [31]:

\[ Y_{n+1} = rY_n (1 - Y_n) \]  \hspace{0.5cm} (1)

Where \( Y_n \) values are in the range [0,1], the \( r \) parameter is defined as positive and it allows values in the range [0,4]. Its utilized value controls and gives the manner of how logistic map can work.

The 2D-CLM is more complicated than the 1D-CLM since it has a complex chaotic manner which makes it efficiently sufficient for data encryption. The 2D-CLM can be mathematically described as [23-24]:

\[
\begin{align*}
    X_{i,t+1} &= r(3Y_i + 1)X_i (1 - X_i) \\
    Y_{i,t+1} &= r(3X_i + 1)Y_i (1 - Y_i)
\end{align*}
\]  \hspace{0.5cm} (2)

Where \( r \) defines system control parameter and \((X_i, Y_i)\) represents pair-wise point at iteration \( i \) th.

B. The SVD

The Singular value decomposition (SVD) is a commonly famous method in linear algebra, and it has many mathematical applications with respect to matrix inversion. The SVD can be considered as a powerful tool in numerical analysis that can be utilized in matrix analysis. The SVD transformation method works by splitting the matrix into three equivalent sized matrices like the input matrix. So, any image may be considered like an array of positive scalar like a matrix. If \( Z \) is a square image, defined like \( Z \in \mathbb{R} \) with size of \( n \times n \), where \( R \) defines the domain of real numbers, then SVD of \( Z \) can be mathematically described as [32]:

\[ Z = USV^T \]  \hspace{0.5cm} (3)

Where \( U \) and \( V \) define the orthogonal vertical and horizontal matrices with condition \( UTU = I \) and \( VTV = I \), where \( I \) defines the identity matrix. \( S = \text{diagonal}(\sigma_1, ..., \sigma_p) \), \( p = \min(m,n) \), \( \sigma_1 \geq \sigma_2 \geq ... \geq \sigma_p \) represent \( Z \) singular values. Diagonal entries may be considered as \( Z \) matrix singular values. The \( U \) columns and \( V \) columns are the \( Z \) left and right singular vectors. The SVD of \( Z \) is mathematically defined like given above in Eq. 3, where \( S \), \( U \) and \( V \) are the diagonal, orthogonal vertical and horizontal matrices.

III. THE PROPOSED 2D-CLM BASED SVD IMAGE CIPHER

The proposed 2D-CLM based SVD image cipher is based on the utilization of 2D-CLM and SVD. The encryption procedure of 2D-CLM based SVD image cipher works through applying the 2D-CLM to the input plainimage. The logistic transformed image is then decomposed with the SVD into the final ciphered diagonal, vertical, and Horizontal orthogonal matrices which then transmitted to the receiving end. The decryption procedure follows the inverse procedure of the encryption. It starts by applying the inverse SVD transformation to the received ciphered diagonal, vertical, and Horizontal orthogonal matrices then followed by applying the inverse 2D-CLM to retrieve the final decrypted image. Figs. 1-2 show the encryption/decryption procedures of 2D-CLM based SVD image cipher, respectively.

IV. SECURITY STUDY

The security investigation of 2D-CLM based SVD image cipher is examined with a matrix of encryption measures and with the visual inspection. The proposed 2D-CLM based SVD image cipher is tested with a group of tests for investigating the performance of the proposed 2D-CLM based SVD image cipher for ciphering gray scale. These tests have been done using a set of different test images; such as Brabra, Boat and Pirate images as shown in Fig. 3.

A. Visual Inspecting Results

The visual inspecting results of encrypting different test images; such as Brabra, Boat and Pirate images using the proposed 2D-CLM based SVD image cipher are in Fig. 4. The visual inspection results show that the proposed 2D-CLM based SVD image cipher can successfully hide all the details of the tested plainimages. These visually inspected results have verified and proved the efficiency of 2D-CLM based SVD image cipher.
B. Histogram Test

The histogram results of examined plainimages and their corresponding cipherimages using the 2D-CLM and the proposed 2D-CLM based SVD image cipher are shown in Fig. 5. The cipherimages histogram results using the proposed 2D-CLM based SVD image cipher are completely different from their corresponding plainimages histogram results. On the other hand, it is noticed that the cipherimages histogram results using the 2D-CLM image cipher are equivalent to their corresponding plainimages histogram results. This is expected since the 2D-CLM just changes the location of pixels.

C. Entropy Metric

The entropy metric is performed for examining the cipherimages produced using the proposed 2D-CLM based SVD image cipher. The entropy metric can be defined as follows [33]:

\[ E = -\sum_{i=1}^{n} P_{r} (x_i) \log P_{r} (x_i) \]  

(4)

Where \( x_i \) defines the \( i^{th} \) point intensity. High entropy values indicate a best ciphering. The obtained entropy test results using the proposed 2D-CLM based SVD image cipher are given in Table I. The entropy test results indicate that entropy of encrypted images with 2D-CLM is higher compared with their corresponding results using the proposed 2D-CLM based SVD image cipher. But this is expected due to the decomposition nature of the SVD.

<table>
<thead>
<tr>
<th>Image</th>
<th>Encrypted image with 2D-CLM and the proposed 2D-CLM based SVD image cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brabra</td>
<td><img src="image1.png" alt="Image" /></td>
</tr>
<tr>
<td>Boat</td>
<td><img src="image2.png" alt="Image" /></td>
</tr>
<tr>
<td>Pirate</td>
<td><img src="image3.png" alt="Image" /></td>
</tr>
</tbody>
</table>

Fig. 4. Obtained Encryption Test Results of using the Proposed the Proposed 2D-CLM based SVD Image Cipher.

<table>
<thead>
<tr>
<th>Image</th>
<th>Original Images Histogram</th>
<th>Histogram results with 2D-CLM and the proposed 2D-CLM based SVD image cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brabra</td>
<td><img src="histogram1.png" alt="Image" /></td>
<td><img src="histogram2.png" alt="Image" /></td>
</tr>
<tr>
<td>Boat</td>
<td><img src="histogram3.png" alt="Image" /></td>
<td><img src="histogram4.png" alt="Image" /></td>
</tr>
<tr>
<td>Pirate</td>
<td><img src="histogram5.png" alt="Image" /></td>
<td><img src="histogram6.png" alt="Image" /></td>
</tr>
</tbody>
</table>

Fig. 5. Histogram test Results of Original/Encrypted Images using the Proposed 2D-CLM based SVD Image Cipher.

D. Encryption Quality Tests

A set of encryption quality tests are performed for investigating the quality of encryption for the obtained cipherimages using the proposed 2D-CLM based SVD image cipher. This set of encryption quality tests may contain correlation coefficients test (Cr), irregular deviation test (Id) and histogram deviation test (Hd).

1. Correlation Coefficients Metric (Cr)

The correlation coefficients test (Cr) is estimated among plainimage/cipherimage as follows [34]:

\[ C_r = \frac{\text{cov}(P,C)}{\sqrt{D(P)}\sqrt{D(C)}}. \]  

(5)

Small Cr values shows high encryption quality.

2. Irregular Deviation Metric (ID)

The ID metric estimate the encryption quality through computing the abnormality resulted by encryption using the proposed 2D-CLM based SVD image cipher. The IR Metric can be calculated as follows [35]:

\[ I_D = \left( \frac{\sum_{i=0}^{255} | h(i) - M_h |}{MxN} \right). \]  

(6)

The achieved correlation coefficients test results for the 2D-CLM and the proposed 2D-CLM based SVD image cipher are given in Table II. The obtained test results show that Cr among plainimage/cipherimage pairs is very small and close to the ideal value of zero that demonstrate high encryption quality.

<table>
<thead>
<tr>
<th>Image</th>
<th>Entropy values with 2D-CLM and the proposed 2D-CLM based SVD image cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2D-CLM</td>
</tr>
<tr>
<td>Brabra</td>
<td>7.43567</td>
</tr>
<tr>
<td>Boat</td>
<td>7.09441</td>
</tr>
<tr>
<td>Pirate</td>
<td>7.2966</td>
</tr>
</tbody>
</table>

TABLE I. ENCRYPTED IMAGES ENTROPY USING THE PROPOSED 2D-CLM BASED SVD IMAGE CIPHER

<table>
<thead>
<tr>
<th>Image</th>
<th>Entropy values with 2D-CLM and the proposed 2D-CLM based SVD image cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2D-CLM</td>
</tr>
<tr>
<td>Brabra</td>
<td>4.8728*10^3</td>
</tr>
<tr>
<td>Boat</td>
<td>-1.4715</td>
</tr>
<tr>
<td>Pirate</td>
<td>-919*10^5</td>
</tr>
</tbody>
</table>

TABLE II. CORRELATION COEFFICIENT TEST RESULTS USING THE PROPOSED 2D-CLM BASED SVD IMAGE CIPHER
is the ideal encrypted histogram. Small

\[ j = \begin{cases} 1 & \text{if } E_1(x_i, y_j) = E_2(x_i, y_j) \\ 0 & \text{Otherwise} \end{cases} \]

The HD metric can be estimated as follows [36]:

\[ H_D = \frac{\sum_{i=0}^{255} d(i)}{M \times N}, \]  

Where \( d(i) \) defines the difference between plainimage/cipherimage pairs at pixel intensity \( i \). \( M \) and \( N \) represent the image height and width. Higher ID values demonstrate good quality for encryption. The HD test results for both the 2D-CLM and the proposed 2D-CLM based SVD image cipher are given in Table III. It is noticed that the obtained HD values using the 2D-CLM image cipher is zero. This can be interpreted since the 2D-CLM image cipher is just shuffle pixels position and does not change the histogram after employing the encryption. So, it is expected theoretically that the HD values using the 2D-CLM image cipher is zero. Also, results demonstrated that the values of HD using the proposed 2D-CLM based SVD image cipher are high compared with the obtained ID values using the 2D-CLM image cipher. This again confirmed the efficiency of the proposed 2D-CLM based SVD compared with the 2D-CLM.

### Table III. Irregular Deviation Test Results Using the Proposed 2D-CLM Based SVD Image Cipher

<table>
<thead>
<tr>
<th>Image</th>
<th>Irregular deviation values with 2D-CLM and the proposed 2D-CLM based SVD image cipher</th>
<th>2D-CLM</th>
<th>2D-CLM</th>
<th>2D-CLM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S</td>
<td>V</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>Brabra</td>
<td>232.231 \times 10^3</td>
<td>168.86 \times 10^3</td>
<td>168.800 \times 10^3</td>
<td>168.861 \times 10^3</td>
</tr>
<tr>
<td>Boat</td>
<td>203.3 \times 10^3</td>
<td>220.92 \times 10^3</td>
<td>220.90 \times 10^3</td>
<td>220.924 \times 10^3</td>
</tr>
<tr>
<td>Pirate</td>
<td>234.3 \times 10^3</td>
<td>191.68 \times 10^3</td>
<td>191.67 \times 10^3</td>
<td>191.68 \times 10^3</td>
</tr>
</tbody>
</table>

Where \( h(i) \) is cipherimage histogram at the \( i \) intensity value, and \( M \), \( N \) are the ideal encrypted histogram. Small ID values demonstrate a good encryption quality.

The ID test results of both the 2D-CLM and the proposed 2D-CLM based SVD image cipher are given in Table III. The achieved testing results showed that the ID values using the proposed 2D-CLM based SVD image cipher are good when compared to their corresponding ID values using the 2D-CLM image cipher. This confirmed the efficiency of the proposed 2D-CLM based SVD compared with the 2D-CLM.

### D3. Histogram Deviation Metric (HD)

The HD Metric estimate computes the encryption quality through measuring the variation increase between plainimage \( (P) \) cipherimage \( (C) \) pairs. The HD metric can be estimated as follows [36]:

\[ H_D = \frac{\sum_{i=0}^{255} d(i)}{M \times N}. \]  

Where \( d(i) \) defines the difference between plainimage/cipherimage pairs at pixel intensity \( i \). \( M \) and \( N \) represent the image height and width. Higher ID values demonstrate good quality for encryption. The HD test results for both the 2D-CLM and the proposed 2D-CLM based SVD image cipher are given in Table IV. It is noticed that the obtained HD values using the 2D-CLM image cipher is zero. This can be interpreted since the 2D-CLM image cipher is just shuffle pixels position and does not change the histogram after employing the encryption. So, it is expected theoretically that the HD values using the 2D-CLM image cipher is zero. Also, results demonstrated that the values of HD using the proposed 2D-CLM based SVD image cipher are high compared with the obtained ID values using the 2D-CLM image cipher. This again confirmed the efficiency of the proposed 2D-CLM based SVD compared with the 2D-CLM.

### Table IV. Histogram Deviation Test Results Using the Proposed 2D-CLM Based SVD Image Cipher

<table>
<thead>
<tr>
<th>Image</th>
<th>Irregular deviation values with 2D-CLM and the proposed 2D-CLM based SVD image cipher</th>
<th>2D-CLM</th>
<th>2D-CLM</th>
<th>2D-CLM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S</td>
<td>V</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>Brabra</td>
<td>0</td>
<td>415.884 \times 10^3</td>
<td>372.537 \times 10^3</td>
<td>416.072 \times 10^3</td>
</tr>
<tr>
<td>Boat</td>
<td>0</td>
<td>396.661 \times 10^3</td>
<td>374.782 \times 10^3</td>
<td>396.657 \times 10^3</td>
</tr>
<tr>
<td>Pirate</td>
<td>0</td>
<td>427.85 \times 10^3</td>
<td>374.78 \times 10^3</td>
<td>428.04 \times 10^3</td>
</tr>
</tbody>
</table>

E. Differential Metrics

Differential metrics are employed for testing the effect of one pixel modification in the input plainimage on the resulted cipherimage using 2D-CLM based SVD image cipher. Differential metrics may include both the Unified Average Changing Intensity (UACI) and the Number of Pixels Change Rate (NPCR) metrics. The NPCR calculates the percentage of unequal pixels in two ciphered images \( E_1 \) and \( E_2 \). The NPCR can be computed as follows [37-39]:

\[ NPCR(E_1, E_2) = \frac{\sum_{i,j} D(x_i, y_j)}{M \times N} \times 100\%, \]  

\[ D(x_i, y_j) = \begin{cases} 1 & \text{if } E_1(x_i, y_j) = E_2(x_i, y_j) \\ 0 & \text{Otherwise} \end{cases} \]  

Where \( M, N \) represent both the \( E_1 \) and \( E_2 \) height and width.

The UACI evaluates the variance average intensity among two encrypted images, \( CE_1 \) and \( CE_2 \) The UACI can be computed as [37-39]:

\[ UACI(CE_1, CE_2) = \frac{1}{M \times N} \left[ \sum_{i,j} CE_1(x_i, y_j) - CE_2(x_i, y_j) \right] \times 100\%. \]  

The results of NPCR and UACI between two cipherimages with a modification in one-pixel in their respected plainimages using the proposed 2D-CLM based SVD image cipher are given in Table V. The NPCR and UACI evaluations prove that the proposed 2D-CLM based SVD image cipher is sensitive to tiny changes in the tested images which indicate a good encryption.

### Table V. NPCR/UACI Test Results Using the Proposed 2D-CLM Based SVD Image Cipher

<table>
<thead>
<tr>
<th>Image</th>
<th>Irregular deviation values with 2D-CLM and the proposed 2D-CLM based SVD image cipher</th>
<th>2D-CLM</th>
<th>2D-CLM</th>
<th>2D-CLM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S</td>
<td>V</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>Brabra</td>
<td>NCPR</td>
<td>99.3606</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>UACI</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Boat</td>
<td>NCPR</td>
<td>99.0112</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>UACI</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Pirate</td>
<td>NCPR</td>
<td>99.2935</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>UACI</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

V. Conclusions

The paper presented an efficient and secure 2D-CLM based SVD image cipher. The proposed 2D-CLM based SVD image cipher is inspected, examined and investigated with a group of different encryption quality metrics such as visual inspecting, histogram examination, entropy testing, encryption quality measures and differential testing. The obtained test outcomes proved the superiority and affectivity of 2D-CLM based SVD image cipher in terms of different encryption quality metrics.

---

www.ijacsa.thesai.org
REFERENCES


www.ijacsasai.org